Generate custom wordlist

Cracking passwords is good to know.

If we are able to do a dictionary-attack against a service it is important that we use a good dictionary. We can use e generic one. But we can also generate a custom wordlist based on certain criteria. That is what we are going to do in this chapter.

Remember people often use their birth dates, address, street address, pets, family members, etc.

Who is the target?

The target might be a specific company or person.

Password rules

The service you want to hack might have specific password rules. Must contain certain characters, must be of certain length etc.

Combine a small/semi-small dict with a custom

To combine two wordlists you can just do

```
cat wordlist.txt >> wordlist2.txt
```

Create a custom wordlist

Html2dic - Build dictionary from html

You can build a dictionary from a html-page.

```
curl http://example.com > example.txt
```

Then run:

```
html2dic example.txt
```

Then you should probably remove duplicates.

Cewl - Spider and build dictionary

```
cewl -w createWordlist.txt https://www.example.com
```

Add minimum password length:

```
cewl -w createWordlist.txt -m 6 https://www.example.com
```

Improve the custom wordlist

As we all know few password are just simple words. Many use numbers and special characters. To improve our password list we can use john the ripper. We can input our own rules, or we can just use the standard john-the-ripper rules

```
john ---wordlist=wordlist.txt --rules --stdout > wordlist-modified.txt
```

References

http://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-4-creating-custom-wordlist-with-crunch-0156817/